Enterasys Dragon-EAL™ Intrusion Defense System

Security Target

Version 11
August 31, 2004

Enterasys Networks
50 Minuteman Road
Andover Massachusetts 01810
www.enterasys.com

Table of Contents

Table of Tables

Table of Figures

1. Security Target (ST) Introduction

This section identifies the Target of Evaluation (TOE) and the Security Target for the TOE. It contains conformance claims, provides an overview of the ST, describes the ST organization, identifies document conventions, and presents terminology used in this document.

1.1 Identification

TOE Identification:

Enterasys Dragon-EAL™ Intrusion Defense System[1] version 1.0

The Dragon-EAL consists of the Dragon IDS™ v6.3 software which can reside in one of two hardware models. Models are offered with different physical media types and performance rating, but this does not affect or differentiate the security functions in any way. The physical interfaces are functionally identical across all of the models. These models are identified as follows:

Dragon-EAL-TX
Dragon-EAL-SX
Dragon-E500-TX
Dragon-E500-SX

Dragon-EAL-TX/SX consists of:
Either the DSNSA-GE250-TX or SX appliance, Dragon software version 6.3, DSEMS (EMS Software license)

Dragon-E500-TX/SX consists of:
Either the DSNSA-GE500-TX or SX appliance, Dragon software version 6.3, DSEMS (EMS Software license)

TX versions contain dual port Copper gigabit interface

- SX versions contain dual port Fiber gigabit interface
- EAL-TX and SX perform at 250 Megabits per second
- E500-TX and SX perform at 500 Megabits per second

For the purpose of this ST, all of these models are referred to as Dragon-EAL.

CC Identification: Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999) Part 2 and Part 3
International interpretations with effective dates on or before March 27, 2003. This includes the following international interpretations: 003, 051, 065, 141, and 202.

ST Identification: Enterasys Dragon-EAL™ Intrusion Defense System Security Target

ST Date: August 31, 2004

ST Version: 11

[1] Also to be called the Dragon-EAL Intrusion Detection System or the Dragon-EAL IDS.

1.2 TOE Overview

The TOE is a self-contained, appliance-based Intrusion Defense System with host-based and network-based sensors as well as management, and reporting features. It is a commercial off the shelf (COTS) product manufactured by Enterasys Networks. Features of this TOE describe an Intrusion Detection System capability including the following:

- Integrated network based intrusion detection, host-based intrusion detection, and enterprise management
- Cross technology security monitoring of third-party routers, switches, firewalls, applications, web servers, and even other intrusion detection products
- Centralized policy management, analysis, and reporting using Dragon Enterprise Management Server
- High visibility into the state of the network with real-time reporting and historical forensics
- Executive-level reporting with summarized, printable network security reports for easy interpretation
- Multi-method detection including pattern matching, protocol decoding, and anomaly detection
- Large signature base can be updated continuously and posted regularly for detection of new attacks immediately after threat becomes known

1.3 Conformance Claims

- The TOE is Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999) Part 2 extended and Part 3 conformant at EAL2.
- The TOE is also compliant with all International interpretations with effective dates on or before March 27, 2003, as well as interpretations 141 and 202. This TOE is not conformant to any PP[2].

1.4 ST Organization

This ST contains the following sections

- Security Target Introduction (Section 1) – Provides identification of the TOE and ST, conformance claims, this overview of the content of the ST, document conventions, terminology, and an overview of the TOE
- TOE Description (Section 2) – Provides a description of the TOE components and IT security features as well as the physical and logical boundaries for the TOE
- TOE Security Environment (Section 3) – Describes the threats, organizational security policies, and assumptions pertaining to the TOE and the TOE environment
- TOE Security Objectives (Section 4) – Identifies the security objectives for the TOE and its supporting environment as well as a rationale that objectives are sufficient to counter the threats identified for the TOE

[2] While not conformant to the Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.4, February 4, 2002, this ST is based on that PP.

- TOE Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as the rationale for security requirements, security requirements dependencies, and strength of function claim
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements and the measures provided to meet the Security assurance requirements for the TOE as well as the assurance measures and the assurance measures rationale
- Protection Profile Claims (Section 7) – Presents the rationale concerning compliance of the ST with Protection Profile (PP) conformance (if any).
- Rationale (Section 8) – Provides pointers to all rationale sections, to include the rationale for the selection of IT security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability

1.5 Conventions

1.5.1 Convention for Operations

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify the operations performed. .

Assignment Made within the ST: **[bold text in square brackets]**

Selection Made within the ST: [underlined text in square brackets]

Refinement Made within the ST: ***[bold italicized text in square brackets]***

Iteration Made within the ST: indicated with a typical CC requirement naming followed by a lower case letter enclosed in square brackets e.g. FAU_SEL.1.1[a]

1.5.2 Other Conventions

- This ST has explicitly stated requirements. These new requirements contain the text _EXP in the requirement name (e.g. IDS_SCP_EXP.1). Where an explicit requirement is a modification of a CC requirement, the name of the modified CC requirement is also included in the explicit requirement name (e.g. FAU_GEN_EXP.1)
- The ST contains modifications to the CC to address CCIMB Interpretations. These are marked with explanatory footnotes.

1.6 Terms

This section describes terms that are used throughout this Security Target.

1.6.1 IDS and CC Terminology

Analyzer data Data collected by the Analyzer functions

Analyzer functions	The active part of the Analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures
Audit Trail	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized
Authentication	To establish the validity of a claimed user or object
Availability	Assuring information and communications services will be ready for use when expected
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons
Evaluation	Assessment of a PP, a ST or a TOE, against defined criteria
IDS component	A Sensor, Scanner, or Analyzer
Information Technology (IT) System	May range from a computer system to a computer network
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource
Intrusion Detection (ID)	Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break ins or attempts either manually or via software expert systems that operate on logs or other information available on the network
Intrusion Detection System (IDS)	A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately

Intrusion Detection System Analyzer (Analyzer)	The component of an IDS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future)
Intrusion Detection System Scanner (Scanner)	The component of an IDS that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System
Intrusion Detection System Sensor (Sensor)	The component of an IDS that collects real time events that may be indicative of vulnerabilities in or misuse of IT resources
IT Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems
Network	Two or more machines interconnected for communications
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error control information, and message
Packet Sniffer	A device or program that monitors the data traveling between computers on a network
Protection Profile (PP)	An implementation independent set of security requirements for a category of TOEs that meet specific consumer needs
Scanner data	Data collected by the Scanner functions
Scanner functions	The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data). In this ST, the component named the Host Sensor provides the scanner functions.
Security	A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences
Sensor data	Data collected by the Sensor functions
Sensor functions	The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data). In this ST, the component named the Network Sensor provides the sensor functions.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE
System data	Data collected and produced by the System functions
System functions	Functions performed by all IDS component (i.e., Analyzer functions, Scanner functions, and Sensor functions)

Target of Evaluation (TOE)	An IT product of system and its associated administrator and user guidance documentation that is the subject of an evaluation
Threat	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE
Vulnerability	Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing

1.6.2 TOE Specific Terminology

The following terminology is ST specific and is provided in addition to the terminology provided above.

Human User	Any person who interacts with the TOE
Authorized User	A user that is allowed to perform IDS functions and access data. All authorized users are administrative in nature.
Root administrator	An authorized administrator who manages the IDS functionality of the TOE from the OS
Authorized Dragon administrator	An authorized administrator who manages the IDS functionality of the TOE from the EMS
Authorized Analyst	An authorized user who can access System data and use EMS analysis tools to access system data
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE

1.6.3 Acronyms

Acronym	Definition
API	Application Program Interface
ASCII	American Standard Code for Information Interchange
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
CI	Configuration Items
CLI	Command Line Interface: In this ST, CLI refers specifically to the ten IDS reporting data manipulation functions that are available to the dragon administrator from the Forensics console and to the root administrator from the operating system. These may also be referred to as command line tools.
CM	Configuration Management
DAC	Discretionary Access Control
DAR	The name of the Enterasys-hardened version of the Linux-based Slackware operating system that is provided with the TOE. There is no expansion.
EAL	Evaluation Assurance Level
EGID	Effective Group ID
EMS	Enterprise Management System
HIDS	Host Intrusion Detection System: in this ST, the Host Sensor
NIDS	Network Intrusion Detection System; in this ST, the Network Sensor
MMI	Man machine interface
OS	Operating System. In this ST, the operating system is DAR. The operating systems contains all OS commands and CLI commands. The operating system is accessible through a command line interface (in the traditional sense).
OSP	Organizational Security Policy
PEM	Privacy Enhanced Mail
SFP	Security Function Policy
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target

2. TOE Description

This TOE is the Dragon-EAL™ Intrusion Defense System (IDS), a self-contained appliance manufactured by Enterasys Networks. The TOE is *an Intrusion Detection System,* which uses scanners and sensors to collect information about target systems and/or networks, and an analyzer component to support interpretation of the data and initiate actions in response to its findings.

The TOE provides integrated network and host intrusion detection. It supports monitoring of routers, switches, firewalls, applications, web servers, the appliance itself, and other intrusion detection products. The Host Sensor monitors activity on the TOE, collecting information about events. The Network Sensor collects network packets from configured network connections. The data collected is processed by analyzer functions. Analysis methods include pattern matching, protocol decoding, and anomaly detection. TOE users called analysts access the collected and interpreted data to do forensic and trending analysis.

The Dragon Enterprise Management System (EMS) provides policy management and centralized management of monitoring data collection and analysis. It provides high visibility into the state of the network and historical forensics. The reporting system provides executive-level reporting with summarized, printable network security reports for easy interpretation. Enterasys frequently updates its IDS signatures. These signature updates can be downloaded from the Enterasys Dragon website automatically from the EMS. When automatic signature updates are enabled, signatures are downloaded through an Internet connection directly to the EMS using HTTPS. Updates are then pushed to the sensors.

2.1 Architecture

The TOE consists of an enclosed hardware appliance with the Enterasys-modified operating system DAR, and the installed single host configuration of the Dragon 6.3 application software. All components are contained on the TOE appliance. The TOE is to be installed in accordance with the installation instructions in the Dragon-EAL Configuration Guide. This ensures that only the functionality necessary for the single host configuration of the Dragon 6.3 software is installed on the system.

The TOE appliance provides ports that support connection to network switches or to networks to be monitored. When a network switch is used, the Dragon-EAL™ monitors traffic from everything attached to the switch.

Figure 2-1: TOE in sample network architecture shows an example of how the TOE could be placed in a target configuration. The TOE can be used by root administrators, who configure and maintain the appliance via the OS, dragon administrators, who configure and maintain the sensors via EMS, and by analysts who can access intrusion detection reporting data via the EMS. This reporting data includes raw data collected from monitored networks and systems as well as the results of analysis of such data. The root administrators can access the TOE from the physically co-located administrative console, using a command-line interface (CLI) to the OS and via SSH. Dragon administrators and analysts access the TOE remotely through encrypted logical connections via the EMS.

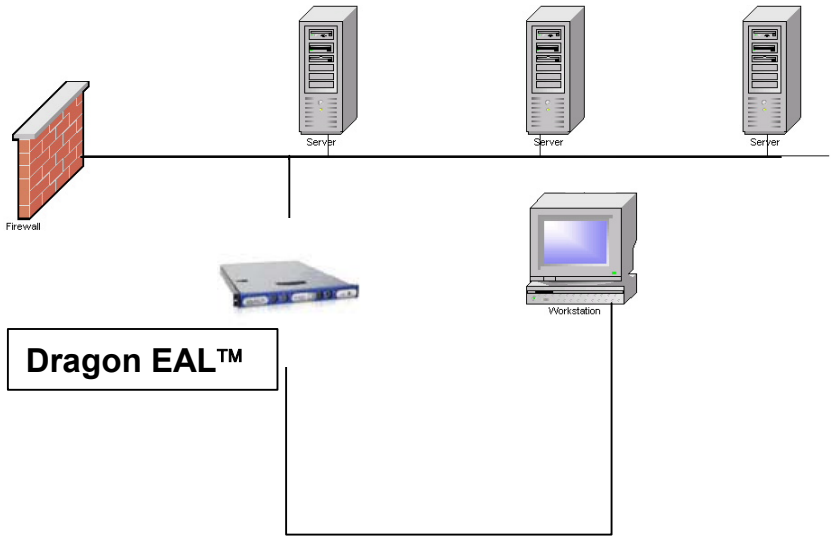

Figure 2-1: TOE in sample network architecture

The administrative network and the network being monitored should be separate networks. The monitoring interface does not have a protocol stack bound to it, therefore it does not have an IP address and is not an active participant in the network. The administrative interface should have an IP address that is not accessible from outside of the organization. This can be accomplished by placing the administrative network behind a firewall or by other means.

Dragon responds in a number of ways from simple administrator notification to automated responses to protect systems. Notification occurs on the administrative network while automated responses occur on the monitored network.

Dragon can utilize a SPAN (switch port analyzer) to monitor network traffic. In order to use the Sniper functionality the SPAN port must be capable of receiving inbound traffic on the SPAN destination port. If the IDS sensor is using a network TAP to receive traffic, the TAP must be capable of allowing the IDS to transparently inject TCP Resets back into the network.

The TOE has a hardware component and two software components. The Software components consist of the Enterasys proprietary operating system DAR, and the Dragon 6.3 application software (e.g., sensors, EMS, and Dragon Agents). Figure 2-2: Dragon-EAL™ Component Architecture shows the hardware and software components of the TOE as well as its potential external physical connections.

Note there is some flexibility in the configuration of the TOE, and the following diagram represents a single instance. This diagram reflects a configuration where OS management is provided by a local terminal, and only one external network is being monitored. Options in configurations are described briefly in the discussion following the diagram.

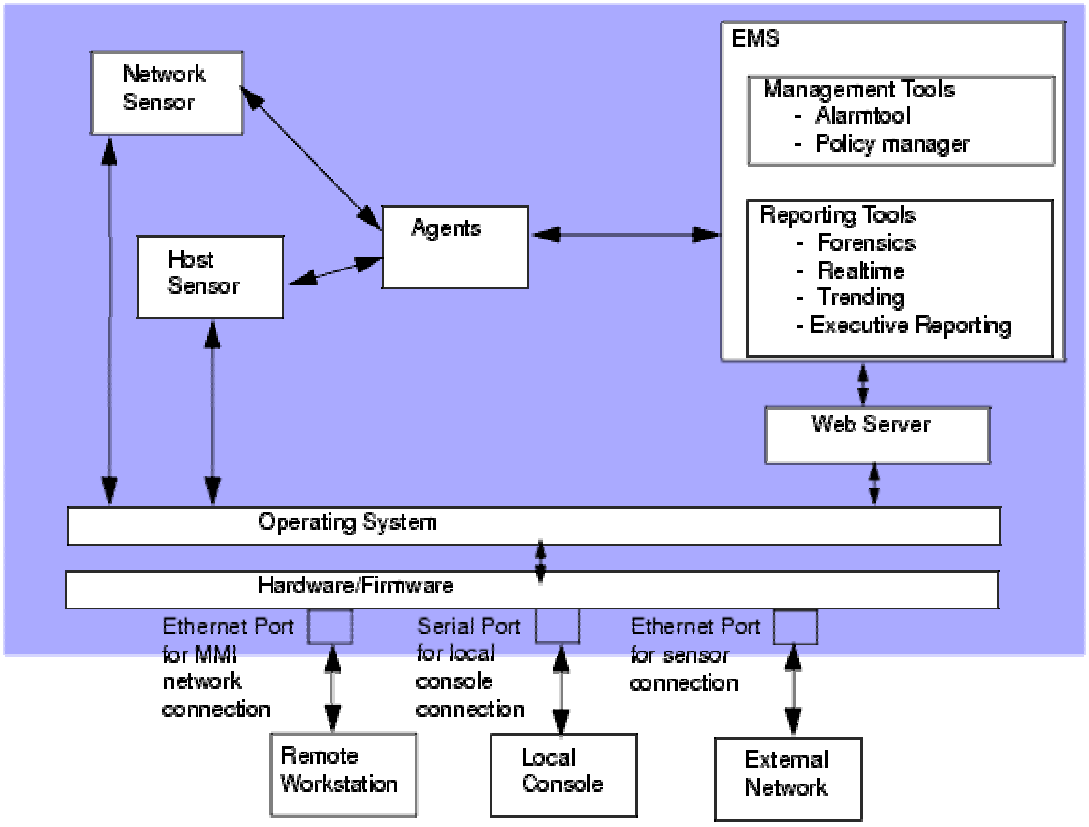

Figure 2-2: Dragon-EAL™ Component Architecture

2.2 Hardware and Firmware

The TOE hardware is an Intel Pentium microcomputer that has one gigabit PCI adapter, two Ethernet ports, two Universal Serial Bus connectors, as well as conventional serial and parallel port connectors, keyboard, mouse, video, timing and memory. The hardware has at least one processor operating at a minimum clock speed of 500 megahertz, at least 512 megabytes of Random Access Memory, and a hard disk storage system of at least 10 Gigabytes.
A local console can be attached to the TOE appliance to provide administrative access to the operating system. This can be a VT100 terminal, a PC running a VT100 emulator, or can be provided by using a mouse, keyboard, and video display directly attached to the TOE hardware. If a VT100 or VT100 emulator is used, it is connected to the hardware via a serial port.

There are Ethernet ports that can be used to provide remote IDS administration and analysis via the web server, remote administration via the operating system, and connection of a network to be monitored by the TOE's IDS functions. One of the Ethernet ports is used for a web-based man-machine interface (MMI) for system management or remote access to the Operating System. Another is used to connect to a network to be monitored by the TOE. Optionally, the third Ethernet port can be used for a connection to a second network to be monitored. The ports are interchangeable. Any port can be used for MMI or network connection; however, it is recommended that the MMI be connected to a management only network.
.

2.3 Software

The software components of the TOE include the Operating system component version 2.1 and the Dragon Application software version 6.3.

2.3.1 Operating System Component

The Enterasys DAR operating system is a hardened version of Slackware, a Linux based product, and is preinstalled on the hardware device. Access to the operating system is provided by a typical command line interface[3]. Administrators can connect to this interface remotely or locally. Local connection is via an attached screen, keyboard, and mouse, or via an attached administrative console that is either a VT100 console or runs under a VT100 emulator. Remote access to the operating system is provided via SSH over the MMI port. The DAR OS components include the following:

- The kernel

  The Linux kernel has been customized to support Symmetric Multi-Processing (SMP). Unneeded drivers have been removed and unneeded services have been disabled.

- Other

  The OS component provides SSH, OpenSSL, Perl, MySQL, and Sendmail. A hardware clock is supported by the operating system component.

2.3.2 Web Server

The TOE uses the Apache Web Server and the Tomcat™ servlet engine as the basis for the tools used to parse and display System data collected by the IDS functions. This supports an effective and intuitive interface for users and administrators to review information on potential events and incidents. The Web Server subsystem is installed on the Dragon-EAL™ appliance.

2.3.3 Dragon Application Software

The components of the Dragon-EAL™ system software are the following:

- Sensors: the TOE provides a network sensor and a host sensor.
- Enterprise Management System (EMS)
- Agents

2.3.3.1 Sensors

- The Host Sensor Component

  The host sensor component is a Host-Based IDS (HIDS) used to monitor activity occurring on the Dragon-EAL™. The Host sensor performs the functions described as scanner functions in the terminology section of chapter 1. The Host Sensor is the component that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of the IT System it monitors. The Host Sensor monitors only the TOE itself (and no remote systems).

[3] Not to be confused with “The CLI”, which is a distinguished set of ten commands discussed in section 6.1.5 and 6.1.6.

Host Sensor events are stored on the appliance and can be analyzed with the analysis and reporting tools. The host sensor component is composed of three engines, the Event Detection Engine (EDE) the Event Filter Engine (EFE), and Event Alerting Engine (EAE). The Host Sensor functionality is implemented by the EDE, EFE, and EAE as well as by other Enterasys-developed modules. The host sensor is capable of the following types of event monitoring: file attribute access and change monitoring, file integrity checking via cryptographic checksums, monitoring the integrity of the Linux kernel, TCP and UDP service initiation and termination, as well as using signatures to monitor file content.

- The Network Sensor Component

  The network sensor component is a packet-based Network IDS (NIDS) that focuses on network performance and the collection of forensic evidence from multiple network connections. It performs the functions defined as sensor functions in the terminology section of chapter 1 and is the component that collects real time events that may be indicative of vulnerabilities in or misuse of IT resources in remote systems it monitors. The network Sensor collects network packets and analyzes them for a variety of suspicious activities, such as detecting IP/TCP/UDP header anomalies, port scan/sweep detection, policy driven events, SNMP alerting, and packet/session reconstruction. It can also match network patterns that may indicate probes, attacks, compromises, and other types of network abuse.

2.3.3.2 Enterprise Management System

The Enterprise Management System (EMS) provides tools that facilitate managing the host and network sensor components of the Dragon-EAL™ IDS and reporting data. Management of the sensor components includes reporting the health of the sensor and allowing security policies to be centrally created and deployed. The EMS allows data collected and interpreted by the sensors to be made available for inspection by dragon administrators and analysts. The information may be log files, summary information, activity graphs, and rebuilt network sessions. The EMS is composed of the following sub-components:

- The Forensics Console

  Provides processing of event data from sensors via web page functionality. It provide such tools as sorting, scoring, and listing of events. The Forensics Console reads information from the Dragon DB. The Dragon Database (Dragon DB)[4] is a set of files with an Enterasys-proprietary format. These files contain forensics-related data received from the host sensor and network sensor (including raw data and analysis results). The Forensics Console is used by dragon administrators to view and process forensics-related data located in the Dragon DB. Root administrators can access Dragon DB forensics information from the OS using the forensics CLI (command line tools).

- The Real-time Consoles

  Provide processing of event data from sensors via web page functionality. It provide such tools as sorting, scoring, and listing events. The real-time console provides a high-speed application using a real-time shell.

- The Trending Console

  The trending console provides a web-based capability to investigate long term trends. The tool uses a program to read collected event data and send it to an SQL database. The Dragon-EAL™ includes schemas and utilities to support the MySQL database. The trending application tools provide quick analysis of event data and long term trending.

[4] The Dragon DB, while a set of files with a proprietary, binary format, can be considered a “proprietary Database.” It is not compliant to any known Database standards.

Because only high-level information is placed into the database, summaries and overall queries happen much quicker than they do with the Forensic and Real time consoles.

- Executive reporting provides high-level reporting capabilities.

  There are eight executive level reports that summarize event counts and distribution of event types over reporting periods of one week.

- Alarmtool.

  The Alarmtool processes events from the ring buffer (or export log), analyzes the event, and possibly initiates delivery of an alert via one or more methods. Alerts can be real-time or summary alerts.

- Policy Manager.

  The Dragon Policy Manager (DPM) is responsible for managing one or more remote sensors. Management of the sensors includes reporting the health of the sensor and allowing security policies to be centrally created and deployed. The DPM is capable of managing both Network and Host Sensors.

2.3.3.3 Dragon Agents

Dragon Agents are software modules that have the ability to process the events.

- MD5Sum Agent

  The MD5Sum agent reads MD5 reference events from Dragon Host Sensor and records them to a local database as well as the Dragon DB. As variances are detected in the enciphered information, the MD5Sum agent records events indicating that the cryptographic value of the specified file has been altered.

- Dragon Database Agent

  Forensics-related data is collected by the host and network sensors in a ring buffer. The Dragon database agent records all packet and event information from the ring buffer to the Dragon DB. The Dragon DB can then be used by the EMS (Forensics Console and Forensics Commands) to view and process reporting data.

- Export Log Agent

  This agent generates an ASCII formatted export log entry for each event. The export log stores only header and event information. The export log information is used to create the MySQL database used by the Trending console of the EMS to create statistical data and reports.

- Alarmtool Agent

  The alarmtool agent processes events, analyzes the event, and may initiate delivery of an alert via one or more methods such as email or page, based on the occurrence of specified events. The Alarmtool Agent is used by the EMS Alarmtool.

2.4 Security Boundaries

This section outlines and describes both the physical and logical security boundaries of the TOE.

2.4.1 Physical Scope and Boundary of the TOE

The TOE is identical to the Dragon-EAL™ appliance. The TOE physical boundary is described in the table below.

Component	TOE or TOE Environment
Dragon-EAL™ version 1 hardware appliance	TOE

Component	TOE or TOE Environment
The DAR operating system version 2.1	TOE
Installed Dragon 6.3 in single server configuration	TOE
Target networks and Systems	TOE Environment
OS Administrative console: VT100 or VT100 emulator, any compatible mouse, screen, and keyboard.	TOE Environment
Remote management and analysis workstations	TOE environment

2.4.2 Logical Scope and Boundary of the TOE

The TOE logical boundary includes the following security services and features:

- Security Audit
- Identification and Authentication and Roles
- Security Management
- TOE Protection
- IDS data collection, analysis, and reaction
- System data management

2.4.2.1 Security Audit

The Security Audit function makes provisions for audit data generation, restricted and selectable audit review. The auditing feature is provided by a combination of functions from the web server, the operating system kernel, and the host sensor. The TOE uses a reliable time stamp mechanism provided by the TOE protection function. This makes it possible to determine the time and order of security relevant events that have been audited.

2.4.2.2 Identification and Authentication and Roles

The Identification and Authentication function is based on user attributes, and ensures that users are identified and authenticated prior to any use of TOE functions. Identification and authentication occurs on the OS or from the web server. Users who are permitted to log into the OS can do this via a local console or remotely via the MMI. Web server users can only log in remotely via the MMI.
Security roles are defined for *Root administrators* who manage the OS, *dragon administrators* who manage the IDS System, and *analysts* who are users authorized to query the system data.

2.4.2.3 Security Management

The security management function contains the functionality to control and manage the IDS and the functionality to control and manage other TOE issues such as system log configurations, accounts and groups. Management and configuration of the IDS system is performed by the dragon administrator via the GUI. Other TOE management is performed by the root administrator from the operating system interface (either via the local console or remotely via the MMI).

2.4.2.4 TOE Protection

The TOE protects itself by providing a domain for its own execution that cannot be accessed by untrusted subjects, and by ensuring that the TSF cannot be bypassed. A TOE execution domain is provided by a combination of physical protection of the TOE, TSF that prevent access by unauthorized users, and lack of visibility to non TOE devices or users as well as entities on the

systems being monitored. Nonbypassability of the TSF is provided by forbidding unauthorized users to access the TOE and by role enforcement.

The TOE provides a reliable time stamp mechanism for its own use.

The TOE also protects communication between analysts or dragon administrators and the TOE using SSL in an HTTPS session. HTTP access is not permitted. OS access can be provided via a local console or remotely. Remote root administrator sessions are protected by SSH.

2.4.2.5 IDS Data Collection, Analysis, and Reaction

The TOE provides both sensor and scanner functionality. The Host Sensor provides data collection and analysis capabilities by scanning selected entities on the TOE. The host sensor observes static data to detect attribute modifications, match signatures, or verify integrity. The Network Sensor provides data collection and data analysis using network traffic from configured remote networks. It provides a variety of signature-based analyses. All data from either sensor is stored in the Dragon DB. The EMS provides tools for further analysis. Selected records are collected and stored in a MySQL database, facilitating statistical analysis at high speed. The Alarmtool send alarms or alerts to the administrator when a likely intrusion is detected by any of the data collecting and analyzing functions.

2.4.2.6 System Data Management

The Intrusion Detection System provides the ability to review the system data via a web interface. system data is available to any administrator or analyst. The IDS also prevents system data loss and ensures of system data availability.

2.4.3 Items not claimed or not in the TOE

The following items are not a part of the TOE.

- Cryptographic algorithms
- Dragon 6.3 software components not included in the single server install.
- Remote hosts and networks being monitored
- SNMP

3. TOE Security Environment

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

3.1.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.1.2 Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.1.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

3.2 Threats

The following threats are identified for the TOE and the IT System that the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

3.2.1 Threats to the TOE

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit System privileges to gain access to the TOE security functions and data.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TSF data or security functions may go undetected.

T.SCNCFG Improper security configuration settings may exist in the TOE.

T.SCNMLC Users could execute malicious code on the TOE which causes modification of the TOE protected data or undermines the TOE security functions.

3.2.2 Threats to the IT System

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan Horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the ST.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, and future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TSF data and functions.

4. TOE Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of the TOE.

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

O.RESPON The TOE must respond appropriately to analytical conclusions.

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

O.OFLOWS The TOE must not overwrite existing data when system data storage is full.

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

O.INTEGR The TOE must ensure the integrity of all audit and System data.

O.EXPORT When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.

O.RMTENC The TOE must protect the confidentiality of its dialog with a remotely connected authorized administrators.

4.2 Security Objectives for the TOE Environment

The TOE operating environment must satisfy the following objectives, which are satisfied by procedural and administrative measures.

O.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

O.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

O.INTROP The TOE is interoperable with the IT System it monitors.

4.3 Rationale for IT Security Objectives

This section provides a rationale for the existence of each assumption, threat, and policy statement that comprise the ST. Table 4.1 Security Environment vs. Objectives demonstrates the mapping between assumptions, threats, and policies to the security objectives is complete. The following discussion provides detailed evidence of the coverage for each assumption, threat, and policy.

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.RMTENC	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP
A.ACCESS																		X
A.DYNMIC																	X	X
A.ASCOPE																		X
A.PROTCT															X			
A.LOCATE															X			
A.MANAGE																	X	
A.NOEVIL														X	X	X		
A.NOTRUST															X	X		
T.COMINT	X						X	X			X							
T.COMDIS	X						X	X				X	X					
T.LOSSOF	X						X	X			X							
T.NOHALT		X	X	X			X	X										
T.PRIVIL	X						X	X										
T.IMPCON						X	X	X						X				
T.INFLUX									X									
T.FACCNT										X								
T.SCNCFG		X																
T.SCNMLC		X																
T.FALACT					X													
T.FALREC				X														
T.FALASC				X														
T.MISUSE			X							X								

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.RMTENC	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP
T.INADVE			X							X								
T.MISACT			X							X								
P.DETECT		X	X							X								
P.ANALYZ				X														
P.MANAGE	X					X	X	X						X		X	X	
P.ACCESS	X						X	X										
P.ACCACT								X		X								
P.INTGTY											X							
P.PROTCT									X						X			

Table 4-1: Security Environment vs Objectives

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

The O.INTROP objective ensures the TOE has the needed access.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

The O.INTROP objective ensures the TOE has proper access to the IT System. The O.PERSON objective ensures that the TOE will be managed appropriately.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The O.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The O.PHYCAL provides for the physical protection of the TOE.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and

will follow and abide by the instructions provided by the TOE documentation.

The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST The TOE can only be accessed by authorized users.

The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TSF data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data. The O.INTEGR objective ensures no TSF data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TSF data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data. The O.EXPORT objective ensures that confidentiality of System data will be maintained. The O.RMTENC objective ensures that confidentiality of dialog with remotely connected authorized administrators. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TSF data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data. The O.INTEGR objective ensures no TSF data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

The O.OFLOWS objective counters this threat by requiring the TOE to not overwrite existing data when system storage is full.

T.FACCNT Unauthorized attempts to access TSF data or security functions may go undetected.

The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

T.SCNCFG Improper security configuration settings may exist in the TOE.

The O.IDSCAN objective counters this threat by requiring the TOE to collect and store static configuration information that might be indicative of a configuration setting change This threat is addressed by the Host Sensor.

T.SCNMLC Users could execute malicious code on the TOE which causes modification of the TOE protected data or undermines the TOE security functions.

The O.IDSCAN objective counters this threat by requiring the TOE to collect and store static configuration information that might be indicative of malicious code This threat is addressed by the Host Sensor.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on

association of IDS data received from all data sources.

The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.

P.MANAGE The TOE shall only be managed by authorized users.

The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

The O.IDAUTH objective provides for authentication of users prior to any TOE

function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

The O.INTEGR objective ensures the protection of data from modification.

P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TSF data and functions.

The O.OFLOWS objective counters this threat by requiring the TOE to not overwrite existing data when system storage is full.
The O.PHYCAL objective protects the TOE from unauthorized physical modifications.

4.4 Rationale for the Security Objectives of the Environment

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

5. TOE Security Requirements

5.1 Security Functional Requirements

This section identifies the functional requirements for the DRAGON-EAL™ IDS VERSION 1.0. Table 5.1 summarizes the functional requirements for the ST. Those requirements not marked in the table with an asterisk were drawn from the CC part 2 functional components. Those requirements marked with an asterisk were created outside of Part 2 of the CC.

Functional Component	Summary Description
FAU_GEN.1	Audit Data Generation
FAU_SAR.1[a] and [b]	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
FAU_STG.1	Protected audit trail storage
FIA_UAU.1	Timing of Authentication
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User Attribute Definition
FIA_UID.1	Timing of Identification
FMT_MOF.1 [a]	Management of Security Functions Behavior: IDS functions
FMT_MOF.1 [b]	Management of Security Functions Behavior: non-IDS functions
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_ITA.1	Inter-TSF Availability Within a Defined Availability Metric
FPT_ITC.1	Inter-TSF Confidentiality During Transmission
FPT_ITI.1	Inter-TSF Detection of Modification
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
IDS_SDC_EXP.1*	System Data Collection
IDS_ANL_EXP.1*	Analyzer Analysis
IDS_RCT_EXP.1*	Analyzer React
IDS_RDR_EXP.1*	Restricted Data Review
IDS_STG_EXP.1*	Guarantee of System Data Availability
IDS_STG_EXP.2*	Prevention of System Data Loss
FAU_STG_EXP.4*	Prevention of Audit Data Loss

Table 5-1: TOE Functional Components

5.2 Security Audit (FAU)

5.2.1 FAU_GEN.1 – Audit Data Generation[5]

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

[5] This requirement has been used in compliance with International Interpretation 202

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) **[The events described in the following table].**

Event	**Details**
Start-up and shutdown of audit functions	
Access to System	
Access/modification to the TSF and System data	Object IDs, Requested access
Reading of information from the audit Records	
All modifications to the audit configuration that occur while the audit collection functions are operating	
All use of the authentication mechanism	User identity, location
All use of the user identification Mechanism	User identity, location
All modifications in the behavior of the Functions of the TSF	
All modifications to the values of TSF data	
Modifications to the group of users that are part of a role	User identity

Table 5-2: Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, and subject identity, and the successful outcome of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**the additional information specified in the Details column of Table 5-2: Auditable Events]**

5.2.2 FAU_SAR.1[a] – Audit Review

FAU_SAR.1.1[a] The TSF shall provide [**Root administrator]** with the capability to read **[all audit information]** from the audit records**.**

FAU_SAR.1.2[a] The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.3 FAU_SAR.1[b] – Audit Review

FAU_SAR.1.1[b] The TSF shall provide **[Analysts, dragon administrators]** with the capability to read [**all audit information in the Dragon DB]** from the audit records.

FAU_SAR.1.2[b] The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.4 FAU_SAR.2 – Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.2.5 FAU_SAR.3 – Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to perform [sorting] of audit data based on [**date and time, subject identity, type of event, and success or failure of related event**.]

5.2.6 FAU_SEL.1 – Selective Audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [Event type;]

b) [No additional attributes]

5.2.7 FAU_STG.1 – Protected Audit Trail Storage[6]

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [detect] unauthorized modifications to the audit records in the audit trail.

5.3 Identification and Authentication (FIA)

5.3.1 FIA_AFL.1 – Authentication Failure Handling

FIA _AFL.1.1 The TSF shall detect when [**3**] unsuccessful authentication attempts occur related to users attempting to authenticate to the TOE. For SSH – After 3 unsuccessful attempts, the session is terminated and a “Failed password” message is written to syslog. For Web – After 3 unsuccessful attempts, the session is terminated and an “Authorization Required” message is generated. For Console– After 3 unsuccessful attempts, an “invalid password” message is written to authlog.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [**delay a short time and then offer the login prompt again for console login. Web login failures remain at the Authorization Required screen until the user reinitiates connection. SSH sessions are terminated and users must reinitiate connection to attempt valid login].**

[6] Changes are made to reflect CCIMB interpretations 141 and 202.

5.3.2 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**User Identity, Authentication data, Authorizations].**

5.3.3 FIA_UAU.1 – Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [**negotiation of an SSH session or HTTPS session and no other actions or activities]** on behalf of the user to be performed before the user is authenticated**.**

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated action on behalf of that user.

5.3.4 FIA_UID.1 – Timing of Identification

FIA_UID.1.1 The TSF shall allow [**negotiation of an SSH session or HTTPS session and no other actions or activities]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.4 Security Management (FMT)

5.4.1 FMT_MOF.1 [a] – Management of Security Functions Behavior: IDS functions[7]

FMT_MOF.1.1 [a] The TSF shall restrict the ability to [modify the behavior of] the functions **[System data collection, analysis, and reaction]** to [**dragon administrators and root administrators.]**

5.4.2 FMT_MOF.1 [b] – Management of Security Functions Behavior: Non-IDS functions[8]

FMT_MOF.1.1 [b] The TSF shall restrict the ability to [determine the behavior or, disable, enable, modify the behavior of] the functions **[the functions listed in the following table]** to [**roles listed in the following table.]**

Function	Authorized user
User account management	Root administrators
Role management	Root administrators
Start up and shut down the system	Root administrators
Set time and date	Root administrators

[7] This requirement has been used in compliance with International Interpretation 065
[8] This requirement has been used in compliance with International Interpretation 065

5.4.3 FMT_MTD.1 – Management of TSF Data[9]

FMT_MTD.1.1 The TSF shall restrict the ability to [**perform the functions as defined in Table 5-3: Management of TSF Data**] the **[TSF data as defined in Table 5-3: Management of TSF Data**] to [**The roles as defined in Table 5-3: Management of TSF Data.]**

Role	Capability	Data
Dragon administrator	Query	System data
Dragon administrator	Query and modify	• configuration and policy data specific to the IDS System
Root administrator	Query	System data and audit data
Root administrator	Query and modify	Any other TSF data including account information and role information
Analyst	Query	System data specific to the IDS
Analyst	Query and modify	None

Table 5-3: Management of TSF Data

5.4.4 FMT_SMF.1 – Specification of Management Functions[10]

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**System data collection, analysis, and reaction, user account management, role management, startup and shut down the system, set the time and date]**

5.4.5 FMT_SMR.1 – Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Root administrator, dragon administrator, and analyst].**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.5 Protection of the TOE Security Functions (FPT)

5.5.1 FPT_ITA.1– Inter-TSF Availability Within A Defined Availability Metric

FPT_ITA.1.1 The TSF shall ensure the availability of [**audit and System data]** provided to a remote trusted IT product within [**60 seconds from when the request was made]** given the following conditions [**the amount of data is 1MB or less and the network traffic conditions are normal].**

5.5.2 FPT_ITC.1– Inter-TSF Confidentiality During Transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

[9] This requirement has been used in compliance with International Interpretation 065
[10] This requirement has been used in compliance with International Interpretation 065

5.5.3 FPT_ITI.1– Inter-TSF Detection Of Modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote IT product within the following metric: [**at least one MAC error in SSL transmissions].**

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [**a re-send of network packet(s) that caused the error]** if modifications are detected.

5.5.4 FPT_RVM.1 – Non-Bypassability Of The TSP

FPT_RVM.1.1 The TSF shall ensure the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.5.5 FPT_SEP.1 – TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects

FPT_SEP.1.2 The TSF shall enforce separation between the security domain of subjects in the TSC.

5.5.6 FPT_STM.1 – Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable stamps for its own use.

5.6 IDS Component Requirements (IDS)

5.6.1 IDS_SDC_EXP.1 – System Data Collection

IDS_SDC_EXP.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) data accesses, service requests, network traffic, security configuration changes

IDS_SDC_EXP.1.2 At a minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity; and

b) The additional information specified in the Details column Table 5-4: System Events

Component	Event	Details
IDS_SDC_EXP.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC_EXP.1	Service Requests	Specific service, source address, destination address
IDS_SDC_EXP.1	Network traffic	Protocol, source address, destination address

Component	Event	Details
IDS_SDC_EXP.1	Security configuration changes	Source address, destination address

Table 5-4: System Events

5.6.2 IDS_ANL_EXP.1 – Analyzer Analysis

IDS_ANL_EXP.1.1 The System shall perform the following analysis function(s) on all IDS data received: signature analysis and/or integrity analysis. The System can also perform trending analysis based on System data collected and stored in the TOE.

IDS_ANL_EXP.1.2 The System shall record within each analytical result at least the following information:
a) Date and time of the result, type of result, identification of data source.

5.6.3 IDS_RCT_EXP.1 – Analyzer React

IDS_RCT_EXP.1.1 The System shall send an alarm to Enterprise Management System and notify an authorized administrator via email or log the intrusion or terminate the session or connection when an intrusion is detected.

5.6.4 IDS_RDR_EXP.1 – Restricted Data Review

IDS_RDR_EXP.1.1 The System shall provide analysts with the capability to read all System data.

IDS_RDR_EXP.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR_EXP.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read access.

5.6.5 IDS_STG_EXP.1 – Protected System data

IDS_STG_EXP.1.1 The System shall protect the stored System data from unauthorized deletion.

IDS_STG_EXP.1.2 The System shall protect the stored System data from modification.

5.6.6 IDS_STG_EXP.2 – Prevention of System data loss

IDS_STG_EXP.2.1 The System shall ignore system data and send an alarm if the TOE storage capacity has been reached.

5.6.7 FAU_STG_EXP.4 – Prevention of Audit Data Loss

FAU_STG_EXP.4.1 The TSF shall prevent auditable events, except those taken by the authorized user, and send an alarm if the TOE storage capacity has been reached.

Note this requirement has a dependency on FAU_STG.1

5.7 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) as defined by the CC with no augmentation. The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5-5: Assurance Requirements: EAL2

5.8 Configuration Management (ACM)

5.8.1 ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.XC The configuration list shall uniquely identify all configuration items that comprise the TOE.[11]

[11] This component was added to comply with international interpretation 003.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.9 Delivery and Operation (ADO)

5.9.1 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.9.2 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE. [12]

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

[12] This component was modified to comply with international interpretation 051.

5.10 Development (ADV)

5.10.1 ADV_FSP.1 Informal Functional Specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.10.2 ADV_HLD.1 Descriptive High-Level Design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.10.3 ADV_RCR.1 Informal Correspondence Demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.11 Guidance Documents (AGD)

5.11.1 AGD_ADM.1 Administrator Guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.11.2 AGD_USR.1 User Guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.12 Tests (ATE)

5.12.1 ATE_COV.1 Evidence Of Coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.12.2 ATE_FUN.1 Functional Testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.12.3 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.13 Vulnerability Assessment (AVA)

5.13.1 AVA_SOF.1 Strength Of TOE Security Function Evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level [***of SOF-Basic]***.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric [***of SOF-Basic].***

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.13.2 AVA_VLA.1 Developer Vulnerability Analysis

Developer action elements:[13]

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:[14]

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

[13] These elements have been modified to comply with interpretation 051.
[14] These elements have been modified to comply with interpretation 051.

5.14 Rationale for TOE Security Requirements

This section demonstrates that the functional components selected for Dragon-EAL™ ST provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.RMTENC
FAU_GEN.1										X			
FAU_SAR.1 [a] & [b]						X							
FAU_SAR.2							X	X					
FAU_SAR.3						X							
FAU_SEL.1						X				X			
FAU_STG.1	X						X	X	X		X		
FIA_UAU.1							X	X					
FIA_AFL.1								X					
FIA_ATD.1								X					
FIA_UID.1							X	X					
FMT_MOF.1 [a]	X						X	X					
FMT_MOF.1 [b]	X						X	X					
FMT_MTD.1	X						X	X			X		
FMT_SMF.1							X						
FMT_SMR.1								X					
FPT_ITA.1												X	
FPT_ITC.1											X	X	X
FPT_ITI.1											X	X	
FPT_RVM.1	X					X		X		X	X		
FPT_SEP.1	X					X		X		X	X		

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.RMTENC
FPT_STM.1										X			
IDS_SDC_EXP.1		X	X										
IDS_ANL_EXP.1				X									
IDS_RCT_EXP.1					X								
IDS_RDR_EXP.1						X	X	X					
IDS_STG_EXP.1	X						X	X	X		X		
IDS_STG_EXP.2									X				
FAU_STG_EXP.4									X	X			

Table 5-6: Requirements vs. Objectives Mapping

The following discussion provides detailed evidence of coverage for each security objective.

O.PROTCT The TOE must protect itself from unauthorized modification and access to its functions and data.

The TOE is required to protect the audit data from deletion. [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion, and guarantee the availability of the data in the event of storage exhaustion [IDS_STG_EXP.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1 [a] and [b]]. Only dragon administrators and root administrators may query and add system and audit data, and root administrators of the TOE may query and modify all other TSF data [FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference preventing it from performing its functions [FPT_SEP.1].

O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of the TOE.

The TOE itself is one of the IT systems that the System monitors. The type of information collected for the TOE by the scanner function (host sensor) is security configuration changes [IDS_SDC_EXP.1].

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse,

access, or malicious activity of IT System assets and the IDS.

The Sensor (Network Sensor) is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. [IDS_SDC_EXP.1].

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

The Analyzer is required to perform intrusion analysis and generate conclusions based on the information collected by the scanner (Host Sensor) and the Sensor (Network Sensor). [IDS_ANL_EXP.1].

O.RESPON The TOE must respond appropriately to analytical conclusions

The TOE is required to respond appropriately if an intrusion is detected [IDS_RCT_EXP.1].

O.EADMIN The TOE must include a set of functions allowing effective management of its functions and data.

The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1 [a] and [b], FAU_SAR.3, FAU_SEL.1]. The System must provide the ability for root administrators to view all system data collected and produced [IDS_RDR_EXP.1]. The TOE must ensure all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The system is required to restrict the review of system data to those granted with explicit read-access [IDS_RDR_EXP.1]. The TOE is required to protect the audit data from deletion [FAU_STG.1]. The system is required to protect the system data from any modification and unauthorized deletion [IDS_STG_EXP.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1 [a] and [b]]. Only dragon administrators and root administrators may query and add system and audit data, and only root administrators of the TOE may query and modify all other TSF data [FMT_MTD.1]. The TOE is required to provide these functions [FMT_SMF.1]

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The system is required to restrict the review of system data to those granted with explicit read-access [IDS_RDR_EXP.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.1]. The system is required to protect

the system data from any modification and unauthorized deletion [IDS_STG_EXP.1]. Security attributes of subjects used to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1, FIA_AFL.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1 [a] and [b]]. Only dragon administrators and root administrators may query and add system and audit data, and root administrators of the TOE may query and modify all other TSF data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles existing for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

O.OFLOWS The TOE must not overwrite existing data when system data storage is full.

The TOE is required to protect the audit data from modification and unauthorized deletion [FAU_STG.1]. The TOE must prevent the loss of audit data if TOE storage space is exhausted [FAU_STG_EXP.4] and shall prevent system data loss when the TOE storage space is exhausted [IDS_STG_EXP.2]. The system is required to protect the system data from any modification and unauthorized deletion [IDS_STG_EXP.1]. When system capacity if full, only the root administrator can access the TOE. The root administrator must make room on the system before data processing can continue.

O.AUDITS The TOE must record audit records for data accesses and use of the system functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU_SEL.1]. The TOE must prevent the loss of collected data if its audit trail is full [FAU_STG_EXP.4]. The TOE must ensure all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

O.INTEGR The TOE must ensure the integrity of all audit and system data.

The TOE is required to protect the audit data from unauthorized modification and deletion [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG_EXP.1]. Only dragon administrators and root administrators may query or add audit and system data [FMT_MTD.1]. The system must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure all functions to protect the data is not bypassed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

O.EXPORT When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the system data.

The TOE must make the collected data available to other IT products

[FPT_ITA.1]. The TOE must protect all data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1].

O.RMTENC The TOE must protect the confidentiality of its dialog with a remotely connected authorized administrator.

The TOE protects the confidentiality of dialog and data transmitted from the TSF to a remote authorized administrator (dragon administrators and root administrators) from unauthorized disclosure during transmission [FPT_ITC.1].

5.15 Rationale for Explicitly Stated Requirements

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

A requirement was created specifically to address prevention of audit data loss. The SFR FAU_STG.4 was used as a model for this function. This function addresses the actions to be taken regarding loss of audit data, other than the audit data in the dragon DB, when TOE storage capacity has been reached. The action to be taken regarding loss of audit data that is stored in the Dragon DB is addressed in the SFR IDS_STG_EXP.2, part of the family described above.

5.16 Rationale for IT Security Requirement Dependencies

The ST satisfies all the requirement dependencies of the Common Criteria. Table 5-7 lists each requirement from the ST with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1[a] and [b]	FAU_GEN.1	YES
FAU_SAR.2	FAU_GEN.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	YES
FAU_STG.1	FAU_GEN.1	YES
FIA_AFL.1	FIA_UAU.1	YES
FIA_UAU.1	FIA_UID.1	YES
FMT_MOF.1 [a] and [b]].	FMT_SMR.1 and FMT_SMF.1	YES
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	YES
FMT_SMR.1	FIA_UID.1	YES
FAU_STG_EXP.4	FAU_STG.1	YES

Table 5-7: Requirements Dependencies

5.17 TOE Strength Of Function Claim and Rationale

The minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism is SOF-basic. Specific strength of function metrics are defined for the following requirements:

FIA_UAU.1	Strength of Function shall be demonstrated such that the probability that authentication data can be guessed is no greater than one in one million (000001).

The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified. The evaluated TOE is intended to operate in commercial and DoD low-robustness environments processing unclassified information. The strength of function is in turn consistent with the security objectives described in section 4 of this document.

5.18 Rationale that SFR are internally consistent and mutually supportive

The selected requirements are internally consistent. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- Satisfying all the dependencies as demonstrated in Table 5-7: Requirements Dependencies
- Tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.14 Rationale for TOE Security Requirements
- Including the SFRs FPT_RVM.1 and FPT_SEP.1 to protect the TSF
- Including audit requirements to detect security-related actions and potential attacks
- Including security management requirements to ensure that the TOE is managed and configured securely.

5.19 Rationale for Security Assurance Requirements

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. While the system may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the system will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

6. TOE Summary Specification

6.1 TOE Security Functions

An overview of the TOE Security functions can be seen in section 2.4.2, Logical Scope and boundary of the TOE.

6.1.1 Security Audit

The TOE auditing function is distributed throughout the TOE and provides the following functionality:

Audit Data Collection	Audit data collection is provided by a combination of operating system functions, the web server functions, and functions of the host sensor component.
Audit data storage and protection	Audit data is stored in the TOE and protected by role enforcement. Measures are taken to address auditing in the event of audit data storage exhaustion for all types of audit data. Collection of audit data that is considered IDS data as well is mentioned in this section, to the extent that it applies to the requirements for the audit function. However, to avoid duplication, the details of these functions are provided in section 6.1.5.1, System data collection.
Security Audit Review	Audit data review is provided by access to audit logs using functionality of the operating system and web server software. Review of audit data that is considered IDS data as well is mentioned in this section, to the extent that it applies to the requirements for the audit function. However, to avoid duplication, the details of these functions are provided in section 6.1.6, IDS Data management.
Selective Audit	The auditing system is designed so that auditing can be performed on a selective basis using administratively managed configuration files. Selectability of audit data that is considered IDS data as well is mentioned in this section, to the extent that it applies to the requirements for the audit function. However, to avoid duplication, the details of these functions are provided in section 6.1.6, IDS Data management.

6.1.1.1 Audit Data Collection

FAU_GEN.1.1: Audit data is collected for each of the auditable events specified in section 5.2.1 FAU_GEN.1 – Audit Data Generation and Table 5-2: Auditable Events. The following list identifies each kind of audit event data and describes the audit events that are collected in that type of data.

OS Syslogs	• Start-up and shutdown of the audit functions that are part of the OS (syslog).

	• Access to the TOE via the OS • Access/modification of TSF data on the OS, including viewing audit data stored on the OS • Modifications to the configuration of parts of the audit function found in the OS. • Modifications to security functions found in the OS • Use of identification and authentication mechanisms on the OS • Modification of the groups of users that are part of the role definition for Root administrators
Web server logs	• Start-up and shutdown of the audit functions that are found on the web server. Note that the web logs are started up with the web server, and cannot be disabled. • Access to the TOE via the web server. • Access to / modification of TSF data accessible from the web server • Modifications to the configuration of parts of the audit function found in the web server • Modifications to security functions found in the web server • Use of identification and authentication mechanisms on the web server • Modification of the groups of users that are part of the role definition for analysts and dragon administrators
Host Sensor records. Note that collection of these auditable events is described in detail in section 6.1.5.1	• Start-up and shutdown of the audit functions that are addressed by the host sensor. • Modifications to audit configuration while audit functions are running • Modification of configuration files that control the behavior of the TOE security functions specific to the Host Sensor • Modification of the values of TSF data pertinent to the IDS functionality • Access to / modification of system data • the actions taken when potential audit storage exhaustion is detected

FAU_GEN.1.2. Each audit mechanism described above captures the date and time of the event recorded, the event type and instigator of the event record, and the outcome of the event in terms of success or failure. When access to the system is attempted, the following information is also included in the audit record: identification of the requestor and the nature of the requested access. For identification and authentication attempts to the TOE, via the OS or the web server, both the user identity and the location of the attempted access are recorded in the log record.

6.1.1.2 Audit Data Storage and Protection

The TOE stores and protects all audit data, ensuring it is available for audit review (see section 6.1.1.3). The TOE can prevent unauthorized deletion of audit records, detect modifications to the audit logs, and takes specific measures in event of audit trail storage exhaustion. All audit data are stored on the operating system. The syslogs and web server logs, are stored in flat files on the operating system. These data are protected by role enforcement. The audit data collected by the host sensor is stored in the Dragon database, available in a proprietary binary format that is ready for interpretation. This data is protected by role enforcement.

FAU_SAR.1[a]: Root administrators are able to read all audit records.Syslogs and weblogs are viewed using the *more* command. No other users of the TOE can read the syslogs or web server logs This is ensured by role enforcement which only permit access to syslogs and web logs to *root* administrators. The root administrator uses ordinary OS commands to read these files. The data in the logs is in a readable format.

FAU_SAR1[b]: The audit records stored in the Dragon DB by the host sensor are available to any authorized user of the system (dragon administrators, analysts, and root administrators). The data is accessed via the web server and is presented in a readable format. Root administrators can read this data via commands that are specific to forensics and the web-based Forensics console.

FAU_SAR.2: The role enforcement implemented by the TOE prevents any users who are not explicitly allowed access to specific auditing records from having read access to the records stored in the Dragon DB. This ensures that if a user is not explicitly allowed access, then access is denied.

FAU_STG.1.1. Only the root administrator is able to delete audit records from the TOE. For the audit files stored in flat files on the OS, only *root* administrators are granted any kind of access. Dragon DB records can only be deleted by a *root* administrator. Note that archival and backup of data is not a part of the TOE.

FAU_STG.1.2: The Host Sensor component monitors all audit trail files (syslogs, web server logs and Dragon DB files) on the DRAGON-EAL™. The Host Sensor detects changes in file permissions, file inode values, User ID (UID), Group ID (GID), increase in file sizes, file truncation, file deletion, and changes in file modification time. Modifications to the trail are detected by changes to file modification time.

FAU_STG_EXP.4: The TOE uses the *sysinfo* module in the operating system component to monitor disk space. The root administrator receives an alert from the *sysinfo* module notifying them that a disk utilization threshold has been exceeded. *Sysinfo* is managed from the TOE Management Subsystem. It is the responsibility of a root administrator to determine how to create additional space on the system. The root administrator has the option of sending syslog and web server log audit data to a remote location for storage. Similarly, the root administrator or the dragon administrator can send Dragon DB data to a remote location for storage. If there is insufficient response to the warnings, and the system reaches 0% disk space available, all activities are stopped until such time as the root administrator frees up enough space to restart the system.

6.1.1.3 Security Audit review

FAU_SAR.1 [a] and [b], FAU_SAR.2: as described in the section 6.1.1.2, the TOE provides for audit review by allowing appropriately authorized users read access to the audit files and prohibits unauthorized personnel from having this access.

FAU_SAR.3: All TOE and audit data can be reviewed through a manual sort using the native functionality of the operating system. This includes the function *sort* and *grep.. Grep* is used as a support tool, for the sorting function. In addition, any authorized user of the system can view the audit records in the Dragon DB via the web interface, Web based sorting is modeled directly on the command line tools, providing a *sort* capability.

6.1.1.4 Selective Audit

FAU_SEL.1: The TOE has detailed capabilities defined within the syslog and that allow root administrators to include or exclude specific system-level events from being logged. Dragon

administrators and root administrators create signatures that define Dragon-level events to be logged. Filters include event type, sensor names, Internet Protocol address, date and time of event.

6.1.2 Identification and Authentication and Roles

The functions described in this section include Identification and authentication, as well as Security roles.

Security Roles	The system defines three security roles
Identification and authentication	The TOE offers security-attribute-based login in two ways: • Via the OS login function (using the administrative console directly attached to the appliance or SSH for remote access) • Via the web-based login function

6.1.2.1 Security Roles

FMT_SMR.1: TOE maintains the following roles:

- Root administrators– This role is able to manage the users of the TOE, to view and or modify the configuration of the operating system and to view any TSF data. This role is implemented by the *root* account on the operating system.

- Dragon Administrators: These administrators manage IDS functions of the TOE. This includes the host and network sensor components of the TOE and the IDS functions of the Enterprise Management System. A Dragon administrator account cannot be created without an associated role; if this is attempted, the action is denied and the interface enforces that a role be specified before proceeding with account creation.

- Analysts;. This role is able to view reporting data in the TOE, but is not permitted to modify any information. An analyst account cannot be created without an associated role; if this is attempted, the action is denied and the interface enforces that a role be specified before proceeding with account creation.

Dragon administrators and analysts are the only users of the TOE via the web server, and they can only access the TOE through the web server. For each individual, an account is created with a unique user ID, a password, and role authorizations. Each role is defined by a group of users. Members of the group are authorized to act in the role the group defines.

Root administrators are the only users of the TOE via the OS, and they can only access the TOE through the OS. Users who log into the administrative console have individual accounts.

6.1.2.2 Identification and Authentication

Users can log into the TOE from the Operating System or into the GUI from a network connection via an internal web server. OS login is used for Administration only and the web server is used for access to the Dragon-EAL™ IDS. Login to the operating system can be accomplished in two ways. One is via a locally attached administrative console and the other is remotely, via an SSL connection to the TOE. Login to the GUI is accomplished remotely only via an SSL connection.

The TOE is delivered with two OS accounts. They are *root* and *dragon*. It is not permitted to log into the *dragon* account on the OS. This account is used solely as the account from which the

Dragon software application executes. The *root* account has an initial password that allows an initial login to the system. This account/password is solely for the purpose of installing the system.

The root administrator is the only role that can log into the OS *root* account, and this is only done for the initial installation of the product. As a part of the installation, the root user who installs the system must set up an individual account and password. All subsequent users of the OS must be assigned an individual account and password and must log into their individual accounts. With the exception of the initial login for installation, it is not possible to SSH directly into the *root* account on the operating system. The guidance documents describe how to disable SSH login for the root account. Users in the wheel user group can use sudo to execute certain administrative commands as described in the administrative guidance. The guidance documents strictly forbid sharing OS accounts.

The TOE is delivered with two web server accounts, *dragon-admin,* a dragon administrator account, and *analyst.* Individual accounts can be set up for additional dragon administrators and additional analysts. The guidance documents strictly forbid sharing web interface accounts.

FIA_ATD.1: Users who log into the operating system have individual accounts and security attributes of User ID, password, and authorization use sudo to execute certain root-level commands. The authorization to *sudo* to *root* is controlled by membership in the wheel group of users. While this can be viewed as role enforcement, there are no explicit roles on the OS.

Users who log into the web server have individual accounts and security attributes User Id, password, and the role(s) for which the user is authorized. On the web server, the possible roles are dragon administrator and Analyst.

FIA_UAU.1 and FIA_UID.1: For all OS login via the local console, no actions are allowed prior to identification and authentication of the user. For all remote logins to the OS, only session negotiation on behalf of the user is allowed prior to identification and authentication of the user.

All logins to the Dragon-EAL™ application via the web server allow negotiation of an SSL session on behalf of the user prior to identification and authentication and subsequently allowing any further actions and activities to take place. Roles are assigned to users when the user account is set up, and login is not permitted if there is no associated role for the user.

All passwords must meet minimal password constraints. Password constraints are checked by the operating system for OS accounts, but are not verified by the web server for web server accounts. The default constraints are that a password must have a minimum of eight alphanumeric characters, up to a maximum of 92 characters.

The authentication mechanism is the only security function realized by a probabilistic or permutational security mechanism. The minimum password length for users and administrators is eight characters (with a character set of at least 92 characters), which meets the SOF claim of SOF-basic.

FIA_AFL.1: The TOE provides authentication failure handling. For SSH – After 3 unsuccessful attempts, the session is terminated and a “Failed password” message is written to syslog. For Web – After 3 unsuccessful attempts, the session is terminated and an “Authorization Required” message is generated. For Console– After 3 unsuccessful attempts, an “invalid password” message is written to authlog.

6.1.3 Security Management

The security management features of the TOE are as follows:

Security Functions and their management	These features identify the management functions required for the TOE and how their use is controlled.
Management of TSF data	These functions manage data that is necessary for the TOE to perform its security functions.

6.1.3.1 Security Functions and their management

There are two types of management functions in this TOE. One is the management of the functions that are used to collect, analyze, and react to IDS data. The management of these functions is the domain of the dragon administrator. The other security functions include functions to manage accounts, groups, and other TOE management functions. These functions are the responsibility of the root administrator.

System Data Configuration Management
FMT_MOF.1 [a] and FMT_SMF.1: The behavior of the system data collection, analysis, and reaction functions is controlled by configuration files. The dragon administrator accesses these configuration files by the Policy Manager web interface, which has the ability to modify these configuration files and hence impact or modify the behavior of these functions. The Dragon administrator cannot access the flat files containing the configuration information directly. Only the root administrator can modify the configuration files by accessing and modifying raw data using os commands, but guidance documents state not to do so.

Other TOE Management Functions
FMT_MOF.1 [b] and FMT_SMF.1: The behavior of the security management functions as listed in the FMT_SMF.1 and FMT_MOF.1 [b] are controlled by role enforcement on the use of the functions and on the data they impact. Only root administrators have the capability to manage these functions.

6.1.3.2 TSF Data

FMT_MTD.1: TSF data includes the audit trail, IDS (System) data, configuration files and other files and data necessary to manage the operating system, the IDS functionality, the web server, and the EMS. The activities of the dragon administrator include access (query and add) any reporting data as well as the configuration and policy information for the sensors and other data specific to the IDS System. Root administrators can view and modify any data stored on the TOE. Analysts can view reporting data. All access is controlled by role enforcement.

6.1.4 TOE Protection

The TOE provides secure communication between users of the remote man-machine interface and the TOE. Dragon-EAL™ uses mod_ssl, which provides strong cryptography for communications between the remote user and the Apache web server via the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLSv1). It is based on OpenSSL and provides support for all major security needs through HTTPS. OpenSSH uses OpenSSL for encryption and other support routines but does not use the SSL protocol. OpenSSL is a general purpose cryptographic library that also implements the Secure Sockets Layer (SSL) protocols. This is the component that does all the cryptographic work for OpenSSH.

Encryption is started before authentication, and no passwords or other information is transmitted in the clear. Encryption is also used to protect against spoofed packets. The MAC algorithm is used in SSH protocol version 2 for data integrity protection.

The transmitted data is encrypted to ensure confidentiality. At least one message authentication code (MAC) error is generated for SSl transmissions. This MAC is transmitted with the data to ensure integrity of the transmitted data and provide the ability to detect modifications to the transmitted data. SSL and SSH can resend data if modifications are detected.

The TOE also provides protection for remote administration by an administrator from a remotely connected workstation. This protection is provided by SSH. Transmitted dialogs are encrypted to ensure confidentiality. SSH login is disabled after installation.

The TOE protects itself from untrusted subjects and from bypass of the TSF. In addition, the TOE provides reliable time stamps that are used in both audit records and system data records. The protections are described below.

6.1.4.1 Protection of information in transit

FPT_ITA.1: Analysts request access to reporting data via a remote connection to the web server. Dragon administrators may request other TSF data by the same means. Root administrators may request access to TSF data or functions over a remote connection to the operating system. Once TSF data is requested, the TOE verifies the entity's authorization or rights to access it. Under normal network and system conditions, the TOE will provide the data or a denial within 60 seconds of the request. This timing is provided for requests of 1 MB of data or less.

FPT_ITC.1: Data transmitted between a remote user and the web server is protected from compromise during transmission by SSL. This includes communication between a dragon administrator and the web server, or analysts and the web server. Data transmitted between a remote root administrator and the Operating System interface is protected for confidentiality by SSH.

FPT_ITI.1 System data and other IDS-specific TSF data is protected from modification during transmission by SSL. TSF data in transit between a remote root administrator and the operating system is protected from modification by SSH. Integrity violations are detected if at least one MAC error is found in an SSL transmission. Since SSH uses SSL, this applies to both types of remote connection. If such integrity violations occur, the TOE will re-send of network packet(s) that caused the error.

6.1.4.2 Non-Bypassability of the TSP

FPT_RVM.1: The TSP enforcement functions that must be invoked and succeed before the functions within the TSC are allowed to proceed include the following:

- Identification and authentication: these functions ensure that no unauthorized users can gain access to the TOE.
- Role enforcement prior to access to any Dragon-EAL™ IDS operation: these functions ensure that authorized users only gain access to the functions to which they are authorized.

The apache web server ensures that an analyst cannot alter the URL to reach a web page to which the user‘s role does not have access,. Furthermore, Analysts cannot modify any data. In this implementation, all user accounts have passwords, including the initial account at installation.

6.1.4.3 TSF Domain Separation

FPT_SEP.1: Domain separation is provided by the mechanisms of the TOE that support controlled access to the TOE via identification and authentication mechanisms and by security mechanisms that further restrict and control access to TOE functions for authorized users of the system.

Furthermore, the two identification and authentication interfaces to the TOE that provides access to TSF internal objects are protected in the following ways:

- The TOE is physically protected by its environment, which protects access to the TOE from the local console.
- The I&A interfaces require login, password, and role enforcement which protects access to the TOE from the local console as well as from remote access.

In addition, the TOE processes, administrative processes to manage the TOE, and authorized user processes to view IDS data, are all trusted. The operating system has been hardened to provide only the necessary functionality of the TOE. Therefore, domain separation is maintained. The TOE monitors IT systems on the network in a transparent mode and cannot be seen by non-TOE devices, users, or entities from the monitored networks. The location of the I&A interface to the OS is not known to entities on the monitored systems and no TOE I&A interfaces are known to external, unknown and untrusted subjects. While this does not ensure domain separation, it does provide support to it.

The network being monitored and the administrative network should be separate networks. The monitoring interface does not have a protocol stack bound to it, therefore it does not have an IP address and is not an active participant in the network. The administrative interface should have an IP address that is not accessible from outside of the organization this can be accomplished by placing the administrative network behind a firewall or other means

6.1.4.4 Reliable Time Stamps

FPT_STM.1 The TOE operating system provides internally generated timestamps based on the time firmware installed on the motherboard. These time stamps are used for both audit and system data.

6.1.5 IDS Data Collection, Analysis, and Reaction

The TOE provides intrusion detection functions that include collection of data from sensor and scanner functions as well as analysis functions found within the sensors themselves and the Enterprise Management System.

The Host sensor is used to monitor the TOE itself, providing monitoring of a variety of data. The Network Sensor can detect a variety of suspicious events by monitoring network traffic from a network it is configured to monitor. The EMS provides functionality to view collected data as well as to determine summary information.

6.1.5.1 Data Collection and Analysis by the Host Sensor

IDS_SDC_EXP.1, IDS_ANL_EXP.1: The Host Sensor performs typical scanning activities by monitoring static data that it has been configured to monitor on the Dragon-EAL™. Monitoring can be configured to run at scheduled intervals, or can be persistent. The Host Sensor collects information about data accesses, service requests, and security configuration changes, using scanning, integrity, and signature based analysis techniques.

Scanning activities include the following

- File attributes: File attributes are monitored and events are generated for activities relevant to file permissions, File User ownership, file group ownership, inode values, file deletion, file truncation, file growth, and modification time changes.

- Linux TCP/UDP Service: On Linux platforms, Specific TCP and UDP services can be monitored to generate events as services are started or existing services terminate.

Integrity analysis activities include the following:

- File MD5: Files are monitored for modification by periodically recalculating a file's MD checksum, and comparing it to the stored checksum. Events are logged when changes are detected.
- Linux Kernel: Events will be generated if the Host Sensor detects that any system calls or kernel interrupts have been "hooked"[15] and generates events if hooking is detected.

Signature-based analysis includes the following

- File content: The content of log files can be scanned and if specified signature patterns exist, alarms can be generated and sent to syslog or as configured in the alarmtool. Records describe the results of analysis of the data. System data recorded include the date and time of the event, event type, subject identity, protocol, source address, and destination address. Analysis data includes the date and time of the result, type of result, identification of data source;

6.1.5.2 System Data Collection and Analysis by the Network Sensor

IDS_SDC_EXP.1, IDS_ANL_EXP.1: The network sensor component collects network packets and analyzes them for a variety of suspicious activities. Configuration files control the type of network traffic to be collected and/or processed and where it is to be recorded. The traffic can include search for IP/TCP/UDP header anomalies, port scan/sweep detection, policy driven events, filtering, SNMP alerting, packet/session reconstruction, unique network patterns that may indicate probes, attacks, compromises, and other types of network abuse.

The network sensor can also attempt to reconstruct a fragmented IP packet. The Network Sensor processes reconstructed packets as if the original packet had not been fragmented. In much the same way, the Network Sensor can piece together UDP and TCP packets to monitor portions of sessions.

The Network Sensor provides several different signature based analysis methods. They include the following:

- Resource-based signatures: This usage-based signature assumes that any attack or probe which attempts to exploit a particular network resource will use that resource at some time. A database has specific unwanted actions with a resource, and when there is a match to such an action, an event is recorded.
- Suspicious signatures: these signatures focus on data that should not be present in a type of network session. For example, CGI-BIN attacks tend to run commands on target machines. As these commands or programs do not occur in normal traffic, identifying them may indicate a web attack in progress.
- Server messages: Many times attacks are known, but it is easier to look for them in the return traffic from a server. An example would be seeing a message that an account was closed because of 10 unsuccessful login attempts.
- Indirect signatures: these are network patterns that may indirectly indicate some form of network misuse of system compromise. For example, certain traffic on the network may only occur if some specific other action has taken place.

Recorded events are sorted into event groups, which include the event types:

[15] System call hooking is a common method for rootkits to weaken the kernel by creating back doors. Interrupt hooking is similar.

- Suspicious: Traffic that may have potential security ramifications
- Probe: Attempts to map out a network but not exploit it
- Attacks: Actual known attacks with intent to compromise a server
- Compromise: Evidence of a successful attack
- Vulnerability: Evidence of a known vulnerability
- Trojan: Evidence of an active Trojan horse network program
- Virus: Evidence of an active network virus

The Network Sensor can include raw data (packets) as well as header and event information and the results of analysis of the data. System data recorded includes the date and time of the event, event type, subject identity, protocol, source address, and destination address. Analysis data includes the date and time of the result, type of result, identification of data source. The raw packet(s) that triggered the analysis as well as a dynamic number of follow-on packets are also included.

6.1.5.3 System Data Collection and Analysis by the EMS

IDS_SDC_EXP.1 and IDS_ANL_EXP.1: The EMS Real Time Console and the Forensics console process event data from sensors. They provide such tools as sorting, scoring, and listing events. The two consoles have similar functionality. The Real Time console gets information from the real-time shell while the Forensics console gets information from the Dragon Database. The EMS Trending Console uses a program to read collected event data from a MySQL database. The Trending Console database is composed of high-level and summary events that have been imported from the Dragon Export log into the MySQL database. These export logs are ASCII based and in many cases, in readable form. The Trending Console utilizes SQL queries to build extremely useful web displays of IP addresses, events, or searching for unique event entries. For each Query, the top seven matches over the selected time range are displayed.

6.1.5.4 Reaction to System Data Analysis

IDS_RCT_EXP.1: Reaction to intrusion detection is performed within the EMS by the Alarm tool. As described above, the Host sensor and network sensor collect and analyze data (static files and network traffic) to determine if an intrusion related event has occurred. Information is stored in the event log and/or Dragon DB. The alarmtool reads this file to determine what kind of alert to send. Alerts can be real-time, summary, or dynamic. Real-time alert notification methods are executed immediately when the alert is triggered. Summary alert methods are only executed at a defined interval. A dynamic alert is one that intelligently switches between real-time and summary based on alert frequency. Alerts are sent to the administrator console. Depending on configuration parameters, the alert may take any of the following actions:

- Notify the dragon administrator via email. While the sendmail daemon is not loaded into the TOE, the sendmail binary is used to deliver outbound mail. Inbound mail transmissions are not allowed.
- Log the intrusion in a specified log file
- Perform an active response whereby the session or connection is terminated. This is dependent on the conditions outlined in Section 2.1 for SPAN or TAP.

6.1.6 System Data Management

The system data management security function contains the following components:

System data storage and protection These functions address the protection and storage

System Data Review	of System data This component addresses the means for reviewing and reporting on system data

6.1.6.1 System Data storage and protection

IDS_STG_EXP.1.1, IDS_STG_EXP.1.2. System data can only be deleted or modified from the operating system command line by a root administrator. System data cannot be deleted from the web server interface because there is read-only access to the system data from this interface.

IDS_STG_EXP.2: The TOE will ignore system data if the storage capacity has been reached. The *sysinfo* module in the operating system component is used to alert the dragon administrator when this condition occurs.

6.1.6.2 System Data Review

IDS_RDR_EXP.1: Root administrators can access the dragon DB via CLI commands. Dragon administrators can also access system data via the web interface. Any user who is permitted to act in the analyst role is granted access to the reporting data. The TOE provides event information in Hypertext Markup Language (HTML) format with a “drill-down” capability to view detailed information and hyperlinks to external resources. Figure 6-1: TOE Real-time Reporting Screen is a screen shot showing the “event summary” page from the real-time reporting console.

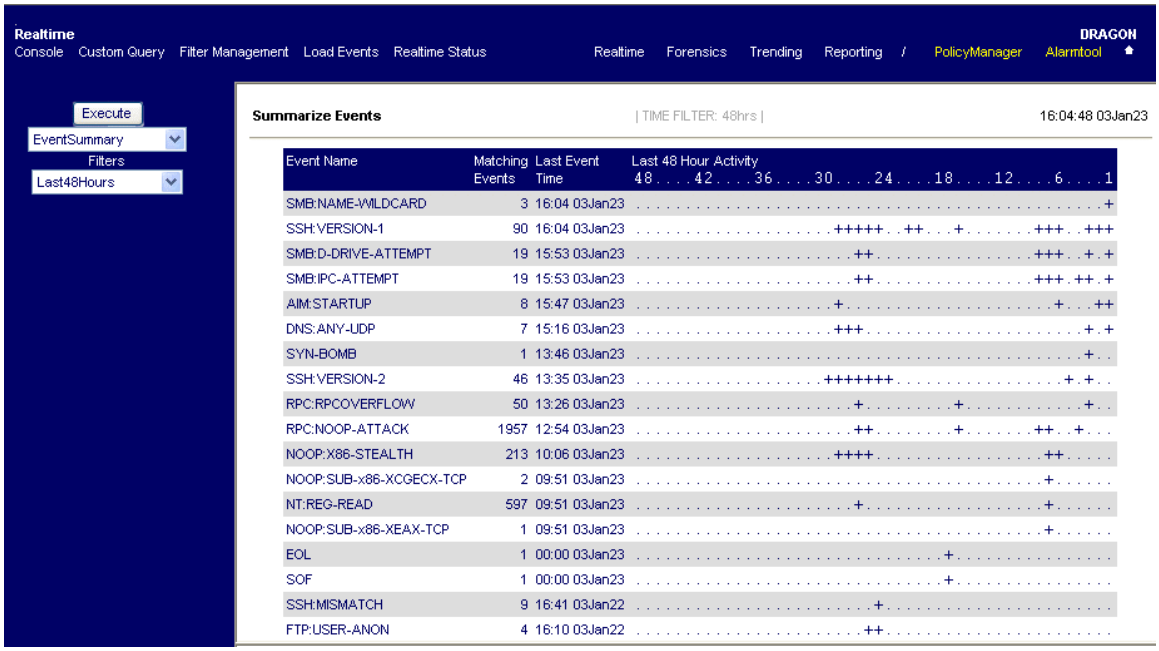

Figure 6-1: TOE Real-time Reporting Screen

6.2 Mapping for TOE Security Functions

The following table represents a mapping between the security functions defined in the TOE Summary specification in this ST to their related TOE security functional requirements and provides a mapping for each security function meets the corresponding security functional requirement. The rationales for the mappings are described in section 6.1.

	Security Audit	Identification & Authentication & Roles	Security Management	TOE Protection	IDS Data Collection, Analysis, and Reaction	System Data Management
FAU_GEN.1	X					
FAU_SAR.1 [a] & [b]	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FAU_SEL.1	X					
FAU_STG.1	X					
FPT_STM.1				X		
FIA_AFL.1		X				
FIA_UAU.1		X				
FIA_UID.1		X				
FIA_ATD.1		X				
FMT_SMR.1		X				
FMT_MOF.1 [a]			X			
FMT_MOF.1 [b]			X			
FMT_MTD.1			X			
FMT_SMF.1			X			
FPT_ITA.1				X		
FPT_ITC.1				X		
FPT_ITI.1				X		
FPT_RVM.1				X		
FPT_SEP.1				X		
IDS_SDC_EXP.1					X	
IDS_ANL_EXP.1					X	
IDS_RCT_EXP.1					X	
IDS_RDR_EXP.1						X
IDS_STG_EXP.1						X
IDS_STG_EXP.2						X
FAU_STG_EXP.4	X					

6.3 Security Assurance Measures

The assurance measures provided by the DRAGON-EAL™ IDS VERSION 1.0. satisfy all of the assurance requirements listed in Section 5.17, Security Assurance Requirements.

6.3.1 Configuration Management (ACM)

ACM_CAP.2 – Configuration Items
Documentation:

- CVS and the Build Process, Revision 1.3, July 22, 2004
- TOE Configuration Listing August 4, 2004

6.3.2 Delivery and Operation (ADO)

ADO_DEL.1 – Delivery Procedures
Documentation:

- Enterasys PLM, Revision J
- Enterasys Engineering Change Order Procedure, Revision Q
- Enterasys Patch Release Process, Revision C
- Order Mgmt Procedure (OE001-H)
- Domestic Shipping Procedure (OTC-SR-006 rev A)
- Enterasys Dragon-EAL Intrusion Defense System Delivery Documentation, Version .3, August 3, 2004

ADO_IGS.1 – Installation, Generation, and Start-Up Procedures
Documentation:

- Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide
- Dragon Intrusion Defense System Version 6.3 Architecture and Installation Guide
- Dragon Intrusion Defense System Version 6.3 Customer Release Notes
- Dragon Intrusion Defense System Version 6.3 Troubleshooting Guide

6.3.3 Development (ADV)

ADV_FSP.1 – Informal Functional Specification
Documentation:

- Enterasys Dragon-EAL™ Intrusion Defense System Functional Specification, version 1.4
- Enterasys Dragon-EAL™ Intrusion Defense System High Level Design, version 1.5
- Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide

ADV_HLD.1 Descriptive High-Level Design
Documentation:

- Enterasys Dragon-EAL™ Intrusion Defense System High Level Design, version 1.5
- Enterasys Dragon-EAL™ Intrusion Defense System Functional Specification, version 1.4
- Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide

ADV_RCR.1 – Informal Correspondence Demonstration Documentation:

- Section 7 of Enterasys Dragon-EAL™ Intrusion Defense System High Level Design, version 1.5
- Section 7 of Enterasys Dragon-EAL™ Intrusion Defense System Functional Specification, version 1.4

6.3.4 Guidance Documents (AGD)

AGD_ADM.1 – Administrator Guidance

Documentation:

- Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide
- Dragon Intrusion Defense System Version 6.3 Host Sensor User's Guide
- Dragon Intrusion Defense System Version 6.3 Network Sensor User's Guide
- Dragon Intrusion Defense System Version 6.3 Enterprise Management Server User's Guide
- Dragon Intrusion Defense System Version 6.3 Troubleshooting Guide
- Dragon Intrusion Defense System Version 6.3 Architecture and Installation Guide

AGD_USR.1 – User Guidance

All users of the TOE are administrative. There are no non-adminstrative interfaces on the TOE. As cited by precedent 0106, this work unit is not applicable to the TOE.
Documentation:

- Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide
- Dragon Intrusion Defense System Version 6.3 Host Sensor User's Guide
- Dragon Intrusion Defense System Version 6.3 Network Sensor User's Guide
- Dragon Intrusion Defense System Version 6.3 Enterprise Management Server User's Guide
- Dragon Intrusion Defense System Version 6.3 Architecture and Installation Guide
- Dragon Intrusion Defense System Version 6.3 Troubleshooting Guide

6.3.5 Tests (ATE)

ATE_COV.1 – Evidence of Coverage
Documentation:

- Dragon-EAL™ Intrusion Defense System SFR to Test Case Mapping, June 21, 2004

ATE_FUN.1 – Functional Testing
Documentation:

- Dragon-EAL™ Intrusion Defense System Test Plan, Version 6.3
- Dragon-EAL™ Intrusion Defense System Test Cases (Bugzilla), Version 2.16.3, June 25, 2004

ATE_IND.2 – Independent Testing (Sample)
Documentation:

- None. The TOE will be supplied to the Common Criteria Test Lab.

6.3.6 Vulnerability Assessment (AVA)

AVA_SOF.1 – Strength of TOE Security Function Evaluation
Documentation:

- Dragon-EAL™ Intrusion Defense System TOE Strength of Function Claim and Analysis, version 1.3, July 16, 2004

AVA_VLA.1 – Developer Vulnerability Analysis
Documentation:

- Dragon-EAL™ Intrusion Defense System Dragon Appliance Vulnerability Assessment, Version 1.4, July 16, 2004

6.4 Rationale for Security Assurance Measures

The assurance documentation listed below was developed to meet the developer action, content, and presentation of evidence elements for each assurance required defined in the CC. The documentation titles in the table below are expected to be updated with new titles and version numbers during the course of the evaluation.

A document entitled Dragon-EAL™ Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide contains pointers to parts of existing documents that are used to meet some documentation requirements.

Assurance Requirement	**Security Assurance Measures**	**Assurance Rationale**
ACM_CAP.2	CVS and the Build Process, Revision 1.3, July 22, 2004 TOE Configuration Listing, Aug 4, 2004	The configuration management document defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.
ADO_DEL.1	Enterasys PLM, Revision J Enterasys Engineering Change Order Procedure, Revision Q Enterasys Patch Release Process, Revision C Order Mgmt Procedure (OE001-H) Domestic Shipping Procedure (OTC-SR-006 rev A) Dragon-EAL Intrusion Defense System Delivery Documentation, v .3, August 3, 2004	The delivery document describes the steps taken to ensure consistent, dependable delivery of the TOE to the customer.

Assurance Requirement	Security Assurance Measures	Assurance Rationale
ADO_IGS.1	Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide Dragon Intrusion Defense System Version 6.3 Architecture and Installation Guide Dragon Intrusion Defense System Version 6.3 Customer Release Notes Dragon Intrusion Defense System Version 6.3 Troubleshooting Guide	The installation, documents describe the steps necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide Enterasys Dragon-EAL™ Intrusion Defense System Functional Specification, v1.4 Enterasys Dragon-EAL Intrusion Defense System High Level Design, v1.5	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.
ADV_HLD.1	Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide Enterasys Dragon-EAL™ Intrusion Defense System Functional Specification, v1.4 Enterasys Dragon-EAL Intrusion Defense System High Level Design, v1.5	The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	Enterasys Dragon-EAL™ Intrusion Defense System Functional Specification, v1.4, Section 7 Enterasys Dragon-EAL Intrusion Defense System High Level Design, v 1.5, Section 7	The informal correspondence document maps the security functionality as described in the FSP to the SFR in the ST and the TOE Summary Specification in the ST. It also contains the mapping of the HLD to the SFR in the ST.

Assurance Requirement	Security Assurance Measures	Assurance Rationale
AGD_ADM.1	Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide Dragon Intrusion Defense System Version 6.3 Architecture and Installation Guide Dragon Intrusion Defense System Version 6.3 Host Sensor User's Guide Dragon Intrusion Defense System Version 6.3 Network Sensor User's Guide Dragon Intrusion Defense System Version 6.3 Enterprise Management Server User's Guide Dragon Intrusion Defense System Version 6.3 Troubleshooting Guide	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	Dragon Intrusion Defense System Dragon-EAL™ Version 1.0 Configuration Guide Dragon Intrusion Defense System Version 6.3 Architecture and Installation Guide Dragon Intrusion Defense System Version 6.3 Host Sensor User's Guide Dragon Intrusion Defense System Version 6.3 Network Sensor User's Guide Dragon Intrusion Defense System Version 6.3 Enterprise Management Server User's Guide Dragon Intrusion Defense System Version 6.3 Troubleshooting Guide	All users of the TOE are administrative. There are no non-adminstrative interfaces on the TOE. As cited by precedent 0106, this work unit is not applicable to the TOE. The user guidance documents provide complete guidance for the TOE user, including all security features.

Assurance Requirement	Security Assurance Measures	Assurance Rationale
ATE_COV.1	Dragon-EAL™ Intrusion Defense System SFR to Text Case Mapping, June 21, 2004	The test coverage document provides a mapping of the test cases performed against the TSF to the SFR.
ATE_FUN.1	Dragon-EAL™ Intrusion Defense System Test Plan, v6.3 Dragon-EAL™ Intrusion Defense System Test Cases (Bugzilla), v2.16.3, June 25, 2004	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort. Expected and actual test results are also provided.
ATE_IND.2	TOE	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_SOF.1	Dragon-EAL™ Intrusion Defense System TOE Strength of Function Claim and Analysis, v1.3, July 16, 2004	The strength of function analysis document provides the SOF argument for the passwords used for administrator login to the TOE.
AVA_VLA.1	Dragon-EAL™ Intrusion Defense System Dragon Appliance Vulnerability Assessment, v1.4, July 16, 2004	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 6-1: Assurance Measure Rationale: EAL2

7. Protection Profile Claims

This ST has no Protection Profile claims.

8. Rationale

8.1 Rationale for IT Security Objectives

The rational for the security objectives is found in section 4.3, Rationale for IT Security Objectives, and in section 4.4, Rationale for the Security Objectives of the Environment.

8.2 Rationale for Security Functional Requirements

The rationale for the security functional requirements is found in section 5.14 , section 5.15, and section 5.16.

8.3 Rationale for security assurance requirements

The security assurance rationale is found in section 5.19.

8.4 TOE Summary Specification Rationale

The TOE Summary specification rationale is found in Sections 6.1, 6.3, and 6.4.

8.5 Protection Profile Rationale

The Protection Profile rationale is found in section 7.

8.6 Rationale for Strength of Function

The Strength of Functions rationale is found in section 5.17.